野田市情報セキュリティポリシー

令和　５年　４月　１日改定

野田市情報セキュリティ委員会了承

目　次

序　情報セキュリティポリシーの構成 ・・・・・・・・・・・・・・・・・・・・・・ 1

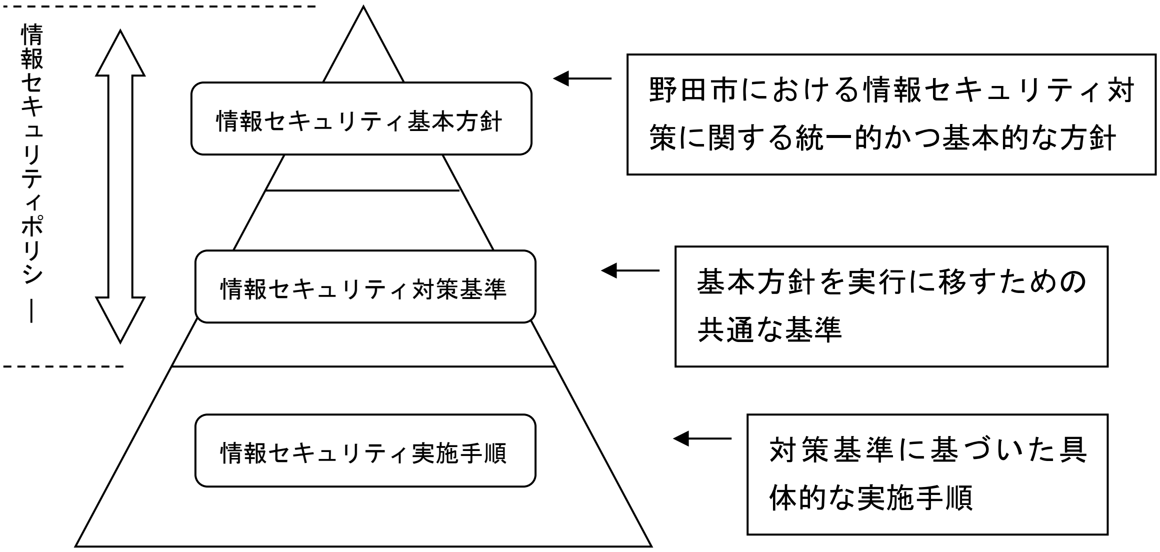
Ⅰ　情報セキュリティ基本方針 ・・・・・・・・・・・・・・・・・・・・・・・・ 2
　１　目的 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　２　定義 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 2
　３　情報セキュリティポリシーの位置付け ・・・・・・・・・・・・・・・・・・ 3
　４　対象範囲 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
　５　責務 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3
　６　情報セキュリティ管理体制 ・・・・・・・・・・・・・・・・・・・・・・・ 3
　７　情報資産の分類 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 4
　８　情報資産への脅威 ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 4
　９　情報セキュリティ対策 ・・・・・・・・・・・・・・・・・・・・・・・・・ 4
　10　情報セキュリティ対策基準の策定 ・・・・・・・・・・・・・・・・・・・・ 5
　11　情報セキュリティ実施手順の策定 ・・・・・・・・・・・・・・・・・・・・ 5
　12　情報セキュリティ監査及び自己点検の実施 ・・・・・・・・・・・・・・・・ 6
　13　評価及び見直しの実施 ・・・・・・・・・・・・・・・・・・・・・・・・・ 6

序　野田市情報セキュリティポリシーの構成

野田市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、野田市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

情報セキュリティポリシーは、野田市が所掌する情報資産に関する業務に携わる全ての者に浸透、普及及び定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層から成るものとして策定することとする。また、情報セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の実施手順として「情報セキュリティ実施手順」を策定することとする。



Ⅰ　情報セキュリティ基本方針

１　目的

　野田市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部への漏えい等が発生した場合には、極めて重大な結果を招く情報が多数含まれている。

　したがって、これらの情報資産及び情報資産を取り扱う情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。ひいては、このことが本市に対する市民からの信頼の維持向上に寄与するものである。

　また、近年のいわゆるＩＴ革命の進展により、電子政府や電子自治体の実現が期待されているところであり、野田市がこれらに積極的な対応をするためには、全ての情報システムが高度な安全性を有することが不可欠な前提条件となる。

　このため、野田市の情報資産の機密性、完全性及び可用性を維持する対策を整備するため、情報セキュリティポリシーを定めることとした。このうち情報セキュリティ基本方針においては、野田市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

２　定義

　情報セキュリティポリシーで使用する用語の定義は、次のとおりとする。

（１）情報セキュリティ

　情報資産の機密性、完全性及び可用性を確保し、維持することをいう。

〈機密性〉　情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

〈完全性〉　情報が破壊、改ざん又は消去されていない状態を確保することをいう。

〈可用性〉　情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（２）行政情報

　業務の執行上、作成又は取得した情報で、情報システムで取り扱う情報（入出力帳票等を含む。）をいう。

（３）情報システム

電子計算機（ネットワーク、ハードウエア及びソフトウエア）及び記録媒体で構成され、業務処理を行う仕組みをいう。

（４）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器をいう。

（５）記録媒体

行政情報の記録や管理に使用される磁気ディスク、磁気テープ、光ディスク等をいう。

（６）情報資産

行政情報及び情報システムをいう。

３　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、野田市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

４　対象範囲

情報セキュリティポリシーが適用される行政機関は、市長、教育委員会、選挙管理委員会、監査委員、公平委員会、農業委員会、固定資産評価審査委員会、水道事業管理者、消防長及び議会並びに野田市土地開発公社(以下「土地開発公社」という。)とする。

５　責務

本市の保有する情報資産を取り扱う職員、非常勤職員、臨時職員等の任用形態、職位及び勤務地を問わず野田市の全ての職員（以下「職員等」という。）は、情報セキュリティの確保を共通の認識とするとともに、情報資産を保護し、かつ、適切に使用するために情報セキュリティポリシー及び関連する法令等を遵守しなければならない。また、情報資産を取り扱う出資法人及び派遣労働者を含む外部委託事業者、指定管理者等（以下「事業者等」という。）に対しても、契約や協定等（以下「契約等」という。）を通じて、情報セキュリティポリシーを遵守させるための措置を講じなければならない。

６　情報セキュリティ管理体制

野田市の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を

確立するものとする。

７　情報資産の分類

情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行うものとする。

８　情報資産への脅威

情報セキュリティポリシーを策定する上で、情報資産を脅かす脅威の発生度合いや発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（１）サイバー攻撃を始めとする部外者の侵入による機器若しくは情報資産の破壊・盗難、故意の不正アクセス又は不正操作による機器若しくは情報資産の破壊・盗聴・改ざん・消去、重要情報の詐取、内部不正等

（２）職員等又は事業者等による脅威
- 機器又は情報資産の持出
- 誤操作
- アクセスのための認証情報又はパスワードの不適切管理
- 設計、開発及びメンテナンスの不備
- マネジメントの欠陥
- 故意の不正アクセス又は不正操作による破壊、盗聴、改ざん、消去等
- 搬送中の事故等による機器又は情報資産の盗難
- 規定外の端末接続によるデータ漏えい等

（３）コンピュータウイルス、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

（４）大規模又は広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）電力供給の途絶、通信の途絶、水道供給の途絶等の提供サービスの障害からの波及等

９　情報セキュリティ対策

上記８で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

（１）人的セキュリティ対策

情報資産に関する権限や責任を定め、職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策や、外部委託等を行う際の情報セキュリティの確保を講ずる。

（２）物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（３）技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス等の不正プログラム対策等を実施する。

（４）運用

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防ぐため、情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講ずるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に緊急時対応として迅速かつ適切に対応を可能とするための対策を講ずる。

10　情報セキュリティ対策基準の策定

野田市の様々な情報資産について、上記９の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

11　情報セキュリティ実施手順の策定

情報セキュリティ対策基準を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公開することにより本市の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。

12　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーが遵守されていることを検証するため、定期的に又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

13　評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。